CLAIMS

1. A method for performing secured communications between a Voice Browser and a network device, said Voice Browser and network device exchanging VoiceXML-based Web content comprising the steps of:

transmitting a request to the network device to establish a secured communication session between the Voice Browser and the network device;

authenticating the network device;

subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;

encrypting the VoiceXML-based Web content using said shared secret as an encryption key;

exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; and,

decrypting the VoiceXML-based Web content using said shared secret as a decryption key.

2. The method of claim 1, wherein said step of authenticating the network device comprises the steps of:

transmitting a digital certificate from the network device to the Voice Browser, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

3. The method of claim 2, wherein said digital certificate is an X.509-compliant digital certificate.

4. The method of claim 1, further comprising the step of authenticating the Voice Browser.

5. The method of claim 4, wherein said step of authenticating the Voice Browser comprises the steps of:

transmitting a digital certificate from the Voice Browser to the network device, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

6. The method of claim 5, wherein said digital certificate is an X.509-compliant digital certificate.

7. The method of claim 2, wherein said step of authenticating the network device further comprises the step of challenging the network device.

8. The method of claim 5, wherein said step of authenticating the Voice Browser further comprises the step of challenging the Voice Browser.

9. The method of claim 7, wherein said step of challenging the network device comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the Voice Browser to the network device;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the Voice Browser.

10. The method of claim 8, wherein said step of challenging the Voice Browser comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the network device to the Voice

Browser;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the network device.

11. The method of claim 1, wherein said negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;

encrypting said generated key with said public key;

transmitting said encrypted key to the network device; and,

decrypting said key in the network device with a private key corresponding to said public key.

12. The method of claim 1, wherein said negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;

encrypting said generated key with said public key;

transmitting said encrypted key to the Voice Browser; and,

decrypting said key in the Voice Browser with a private key corresponding to said public key.

13. The method of claim 1, further comprising the steps of:

exchanging a list of supported symmetrical cryptographic algorithms for the network device and the Voice Browser;

selecting a symmetrical cryptographic algorithm from said list; and,

performing said encrypting and decrypting steps using said selected symmetrical cryptographic algorithm.

14. The method of claim 1, wherein said Voice Browser is a VoiceXML Browser Server.

15. A method for performing secured communications in a Voice Browser comprising the steps of:

transmitting a request from the Voice Browser to a network device for a secure communications session between the Voice Browser and the network device;

receiving from the network device a digital certificate containing a public key and a reference to a certificate authority.

authenticating the network device based on the digital certificate;

subsequent to said authentication, negotiating a shared secret with the network device;

encrypting data using said shared secret as an encryption key and transmitting said encrypted data to the network device; and,

receiving encrypted Web content from the network device and decrypting the Web content using said shared secret as a decryption key.

16. The method of claim 15, wherein said transmitting step further comprises the step of:

transmitting to said network device a list of supported encryption algorithms for use in said encryption and decryption steps,

said network device selecting an encryption algorithm from among said list.

17. The method of claim 16, wherein said data is encrypted using said selected encryption algorithm and said Web content is decrypted using said encryption algorithm.

18. The method of claim 15, wherein said digital certificate is an X.509-compliant digital certificate.

19. The method of claim 15, wherein said Web content is a VoiceXML document.

20. The method of claim 19, wherein said Voice Browser is a VoiceXML Browser Server.

21. A machine readable storage, having stored thereon a computer program for performing secured communications between a Voice Browser and a network device, said Voice Browser and network device exchanging VoiceXML-based Web content, said computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

transmitting a request to the network device to establish a secured communication session between the Voice Browser and the network device;

authenticating the network device;

subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;

encrypting the VoiceXML-based Web content using said shared secret as an encryption key;

exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; and,

decrypting the VoiceXML-based Web content using said shared secret as a decryption key.

22. The machine readable storage of claim 21, wherein said step of authenticating the network device comprises the steps of:

transmitting a digital certificate from the network device to the Voice Browser, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

23. The machine readable storage of claim 22, wherein said digital certificate is an X.509-compliant digital certificate.

24. The machine readable storage of claim 21, for further causing the machine to perform the step of authenticating the Voice Browser.

25. The machine readable storage of claim 24, wherein said step of authenticating the Voice Browser comprises the steps of:

transmitting a digital certificate from the Voice Browser to the network device, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

26. The machine readable storage of claim 25, wherein said digital certificate is an X.509-compliant digital certificate.

27. The machine readable storage of claim 22, wherein said step of authenticating the network device further comprises the step of challenging the network device.

28. The machine readable storage of claim 25, wherein said step of authenticating the Voice Browser further comprises the step of challenging the Voice Browser.

29. The machine readable storage of claim 27, wherein said step of challenging the network device comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the Voice Browser to the network device;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the Voice Browser.

30. The machine readable storage of claim 28, wherein said step of challenging the

Voice Browser comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the network device to the Voice Browser;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the network device.

31. The machine readable storage of claim 21, wherein said negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;

encrypting said generated key with said public key;

transmitting said encrypted key to the network device; and,

decrypting said key in the network device with a private key corresponding to said public key.

32. The machine readable storage of claim 21, wherein said negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;

encrypting said generated key with said public key;

transmitting said encrypted key to the Voice Browser; and,

decrypting said key in the Voice Browser with a private key corresponding to said public key.

33. The machine readable storage of claim 21, for further causing the machine to perform the steps of:

exchanging a list of supported symmetrical cryptographic algorithms for the network device and the Voice Browser;

selecting a symmetrical cryptographic algorithm from said list; and,

performing said encrypting and decrypting steps using said selected symmetrical cryptographic algorithm.

34. The machine readable storage of claim 21, wherein said Voice Browser is a VoiceXML Browser Server.

35. A machine readable storage, having stored thereon a computer program for performing secured communications in a Voice Browser, said computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

transmitting a request from the Voice Browser to a network device for a secure communications session between the Voice Browser and the network device;

receiving from the network device a digital certificate containing a public key and a reference to a certificate authority.

authenticating the network device based on the digital certificate;

subsequent to said authentication, negotiating a shared secret with the network device;

encrypting data using said shared secret as an encryption key and transmitting said encrypted data to the network device; and,

receiving encrypted Web content from the network device and decrypting the Web content using said shared secret as a decryption key.

36. The machine readable storage of claim 35, wherein said transmitting step further comprises the step of:

transmitting to said network device a list of supported encryption algorithms for use in said encryption and decryption steps,

said network device selecting an encryption algorithm from among said list.

37. The machine readable storage of claim 36, wherein said data is encrypted using said selected encryption algorithm and said Web content is decrypted using said encryption algorithm.

38. The machine readable storage of claim 35, wherein said digital certificate is an X.509-compliant digital certificate.

39. The machine readable storage of claim 35, wherein said Web content is a VoiceXML document.

40. The machine readable storage of claim 39, wherein said Voice Browser is a VoiceXML Browser Server.